BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	100 64 720.0
Anmeldetag:	22. Dezember 2000
Anmelder/Inhaber:	timeproof TIME SINGNATURE SYSTEMS GmbH, Hamburg/DE
Bezeichnung:	Authentisierungsmodul
IPC:	H 04 L, G 07 C, G 06 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 5. März 2002
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Wall...

A 9161

Beschreibung

Stand der Technik:

Um die Vorlage digitaler Daten zu einem bestimmten Zeitpunkt nachzuweisen werden digitale Zeitstempel eingesetzt. Diese digitalen Zeitstempel werden durch eine Zeitstempelvorrichtung mittels einer digitalen Signatur gegen Manipulation geschützt. Zur Prüfung der Authentizität des Zeitstempels wird die digitale Signatur verifiziert. Dabei wird eine Verifikation des zur digitalen Signatur gehörenden digitalen Zertifikates, welches von einer Zertifizierungsstelle ausgestellt ist, durchgeführt.

Problem:

Die Zertifizierungsstelle kann nicht immer sicherstellen, dass der zum Zertifikat korrespondierende private Signaturschlüssel nur im Rahmen der Zeitstempelmaschine eingesetzt wird. Wird er ausserhalb der Zeitstempelmaschine benutzt, so können beliebige nicht autorisierte Zeitstempel ausgestellt werden, die sich allerdings nicht von echten unterscheiden lassen.

Beispiel:

Eine Firma verwendet für ihr elektronisches Belegarchiv digitale Zeitstempel als Nachweis für die Archivintegrität. Die Zeitstempel werden ausschließlich von einer hausinternen Zeitstempelvorrichtung ausgestellt. Der zum privaten Schlüssel der Zeitstempelvorrichtung gehörende öffentliche Schlüssel wird von einer Zertifizierungsstelle beglaubigt.

Der Administrator der Firma oder ein Dritter könnte jetzt die Signatureinheit (z.B. PCI-Karte) der Zeitstempelvorrichtung von der Vorrichtung trennen und sie separat betreiben. Da die Signatureinheit alle Daten signiert, die ihr vorgelegt werden, können auch nicht autorisierte Zeitstempel erstellt werden, die nicht von echten unterscheidbar sind.

Vorschlag:

Die Zeitstempelvorrichtung verfügt über ein nicht abtrennbares Authentifizierungsmodul zusätzlich zur Signatureinheit. Jeder Zeitstempel wird nicht nur über die Signatureinheit authentifiziert, sondern auch mittels des Authentifizierungsmoduls. Das Modul verfügt über ein Geheimnis, das eine gültige Authentisierung ausserhalb des Moduls unmöglich macht.

Der Zeitstempel verfügt also neben der digitalen Signatur der Signatureinheit über einen weiteren digitalen Authentifizierungscode.

Vorteile:

Anhand des digitalen Authentifizierungscodes läßt sich nachweisen, ob der Zeitstempel auch tatsächlich mit der Maschine ausgetellt worden ist. Die Möglichkeit nicht autorisierte Zeitstempel auszustellen wird deutlich eingeschränkt.

Beispiel (obiges Szenario):

Wenn ein Angreifer die Signatureinheit von der Zeitstempelvorrichtung abtrennt, so kann er digitale Zeitstempel ausstellen. Allerdings ist er nicht in der Lage den digitalen Authentifizierungscode der Maschine korrekt nachzubilden, denn er verfügt nicht über das Geheimnis des Authentifizierungsmoduls. Der falsche Zeitstempel ist als solcher erkennbar.

Patentansprüche

1. Zeitstempelvorrichtung mit einer Signatureinheit, dadurch gekennzeichnet, daß die Zeitstempeleinrichtung über ein mit der Signatureinheit verbundenes, nicht abtrennbares Authentifizierungsmodul verfügt, wobei jeder Zeitstempel über die Signatureinheit und mittels des Authentifizierungsmoduls authentifizierbar ist.

2. Zeitstempelvorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß das Authentifizierungsmodul über eine geheime Information verfügt, die für eine gültige Authentisierung erforderlich ist.

3. Zeitstempel mit einer digitalen Signatur, die mit der Signatureinheit der Zeitstempelvorrichtung gemäß Anspruch 1 oder 2 erstellt worden ist, dadurch gekennzeichnet, daß der Zeitstempel über einen weiteren digitalen Authentifizierungscode verfügt.